在思科ISE上安装、续订SSL数字证书并对其进行故障排除

目录

简介

本文档介绍SSL证书安装、续订以及针对身份服务引擎上观察到的最常见问题的解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎GUI

使用的组件

本文档中的信息基于以下软件版本：

- 思科身份服务引擎2.7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档提供建议步骤和常见问题核对表，在您开始进行故障排除并致电Cisco技术支持之前，需要验证和解决。

证书是一种电子文档，用于标识个人、服务器、公司或其他实体，并将该实体与公钥相关联。

自签名证书由其自己的创建者签名。证书可由外部证书颁发机构(CA)自签名或数字签名。

CA签名数字证书被视为行业标准，并且更安全。

证书用于网络中，以提供安全访问。

思科ISE使用证书进行节点间通信，以及与外部服务器(例如系统日志服务器、源服务器和所有最终用户门户（访客、发起人和个人设备门户）进行通信。

证书可识别到终端的思科ISE节点并保护该终端与思科ISE节点之间的通信。

证书用于所有HTTPS通信和可扩展身份验证协议(EAP)通信。

本文档提供建议步骤和常见问题核对表，在您开始进行故障排除并致电Cisco技术支持之前，需要验证和解决。

这些解决方案直接来自思科技术支持已解决的服务请求。 如果您的网络处于活动状态，请确保您了解为解决这些问题而采取的步骤的潜在影响。

配置

以下指南介绍如何导入和替换证书：

导入系统证书

https://www.cisco.com/c/en/us/td/docs/security/ise/2-

7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

替换已过期的证书

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

常见问题

场景1：无法在ISE节点上替换到期的门户证书

Error

将新门户证书与CSR绑定时，证书绑定进程失败，错误如下：

内部错误。要求您的ISE管理员检查日志以了解详细信息

此错误的最常见原因包括：

— 新证书与现有证书的使用者名称相同

— 导入使用现有证书的同一私钥的更新证书

解决方案

1. 将门户使用临时分配给同一节点上的另一个证书
2. 删除即将到期的门户证书
3. 安装新的门户证书，然后分配门户使用情况

例如，如果您希望将门户使用临时分配给使用EAP身份验证的现有证书，请执行以下步骤：

步骤1:选择并编辑使用EAP身份验证的证书，在Usage and Save下添加门户角色

第二步：删除即将到期的门户证书

第三步：上传新的门户证书，而无需选择任何角色（在“使用”下）和“提交”

第四步：选择并编辑新的门户证书，在Usage and Save下分配门户角色

方案2：无法为具有多用途使用的同一ISE节点生成两个CSR

Error

使用多用途时为同一节点创建新CSR失败，错误为：
已存在具有相同友好名称的另一个证书。友好名称必须是唯一的。

解决方案

每个ISE节点的CSR Friendly Names都采用硬编码，因此不允许为具有多用途用途的同一节点创建2个CSR。使用案例位于特定节点上，有一个用于管理员和EAP身份验证使用的CA签名证书和另一个用于SAML和门户使用的CA签名证书，并且两个证书都将过期。

在这种情况下：

步骤1:生成第一个具有多用途用途的CSR

第二步：将CA签发的证书与第一个CSR绑定，并分配管理员和EAP身份验证角色

第三步：生成具有多用途使用情况的第二个CSR

第四步：将CA签发的证书与第二个CSR绑定并分配SAML和门户角色

场景3：无法为门户使用绑定CA签名的证书，或者无法将门户标记分配到证书并获取错误

Error

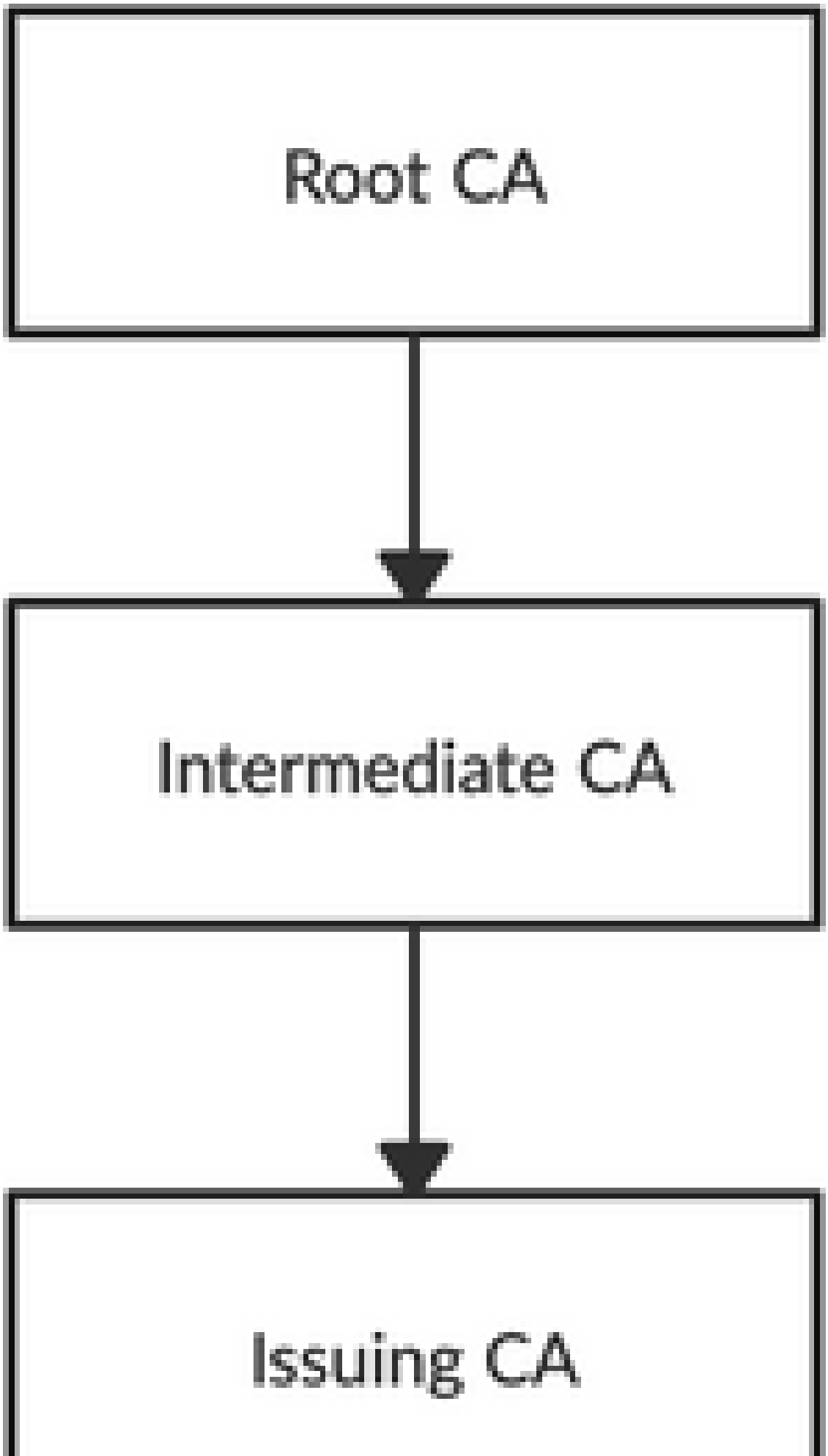
为门户使用绑定CA签名的证书将引发错误：

有一个或多个受信任证书，这些证书是门户系统证书链的一部分，或选择具有基于证书的管理身份验证角色，使用相同的使用者名称但具有不同的序列号。导入/更新已中止。要成功导入/更新，您需要从重复受信任证书禁用基于购物车的管理员身份验证角色，或者从包含其链中的重复受信任证书的系统证书中更改门户角色。

解决方案

步骤1:检查CA签名证书的证书链（用于门户使用）并在受信任证书存储中，验证您是否具有来自证书链的任何重复证书。
第二步：删除重复证书，或者取消选中重复证书中的信任基于证书的管理员身份验证复选框。

例如，CA签名的门户证书具有以下证书链：


Root CA
Intermediate CA
Issuing CA

不允许禁用或删除或信任证书，因为它正在由Remote Logging Targets下的System Certificates AND/OR Secure Syslog Target引用。

解决方案

1. 验证已过期的默认自签名证书未与任何现有远程日志记录目标关联。可以在Administration > System > Logging > Remote Logging Targets > Select and Edit SecureSyslogCollector(s)下验证这一点
2. 验证已过期的默认自签名证书是否未与任何特定角色（用法）关联。可以在管理>系统>证书>系统证书下验证这一点。

如果问题仍然存在，请联系TAC。

场景5：无法将CA签名的pxGrid证书与ISE节点上的CSR绑定

Error

将新的pxGrid证书与CSR绑定时，证书绑定进程失败，错误为：

pxGrid的证书必须在扩展密钥使用(EKU)扩展中同时包含客户端和服务器身份验证。

解决方案

确保CA签名的pxGrid证书必须具有TLS Web服务器身份验证(1.3.6.1.5.5.7.3.1)和TLS Web客户端身份验证(1.3.6.1.5.5.7.3.2)扩展密钥用法，因为它用于客户端和服务器身份验证（以保护pxGrid客户端和服务器之间的通信）

参考链接：https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

方案6：由于现有LDAP或SCEP RA配置文件配置，无法从受信任证书存储中删除已过期的默认自签名证书

Error

从受信任证书存储中删除已过期的默认自签名证书将导致以下错误：

无法删除信任证书，因为它正在其他位置引用，可能来自SCEP RA配置文件或LDAP身份源

*默认自签名服务器证书

要删除证书，请删除SCEP RA配置文件或编辑LDAP身份源以不使用此证书。

解决方案

1. 导航到管理>身份管理>外部身份源> LDAP >服务器名称>连接
2. 确保LDAP服务器根CA未使用“默认自签名服务器证书”
3. 如果LDAP服务器未使用安全连接所需的证书，请导航到管理>系统>证书>证书颁发机构>外部CA设置> SCEP RA配置文件
4. 确保任何SCEP RA配置文件未使用默认自签名证书

其它资源

如何安装通配符证书
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

管理ISE证书
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

在ISE上安装第三方CA证书
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。